REMARKS/ARGUMENTS

Claims 1-32 are pending. In the Office Action, Claims 1-23 and 25-31 were treated as follows.

1. Claims 1-23 and 25-31 under 35 U.S.C. § 102(e) as being unpatentable over Published U.S. Patent App. No. 2003/0046274 to Erickson et al. (hereinafter "*Erickson*").
2. Claims 24 and 32 were objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form.

Applicant acknowledges with appreciation the indication that Claims 24 and 32 recite patentable subject matter. Applicant has respectfully maintained Claims 24 and 32 in dependent form because it is believed that their respective base claims patentably define over the cited art, for at least the reasons discussed herein.

Claim 19 is voluntarily amended not in view of the prior art, but to clarify and more distinctly point out the intended scope of protection. This amendment is discussed in greater detail below.

35 U.S.C. § 102 Rejections

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." MPEP § 2131 (quoting *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)).

***Erickson* overview.**

Applicants respectfully submit that Claims 1-23 and 25-31 are patentable over *Erickson*. *Erickson* is directed towards "a secure container in the form of a universal 'envelope' or meta-container which allows for arbitrary media formats and arbitrary DRM mechanism. This is achieved by attaching… metadata to a secure container containing media content…." ¶ [14]. Thus, *Erickson* seeks to achieve interoperability by use of a standardized file wrapper "whereby a variety of DRM vendors could create 'plug-in' solutions based upon their different value propositions." ¶ [15]. An example from *Erickson* follows:

> reading the external data and determining what, if any, digital rights management mechanism was used to package said content, retrieving or

otherwise accessing an appropriate digital rights management handler accordingly, passing said content through said DRM handler, reading the external data and determining the media handler required to access and handle the content, retrieving or otherwise accessing an appropriate media handler, and passing said content through said media handler.

¶ [12].

Applicants respectfully submit that Claims 1-23 and 25-31 are patentably distinct over *Erickson*. These distinctions will be discussed in more detail below, but in general, *Erickson* generally focuses exclusively on DRM, with no teaching about compression techniques. By contrast, many of the present claims include elements related to compression techniques.

Moreover, Claims 1-23 and 25-31 are directed towards the **en**-cryption of electronic data, whereas *Erickson* is directed towards allowing the **de**-cryption of previously encrypted digital media. For example, *Erickson* discloses that a secure container contains data that has been encrypted, ¶ [13], but *Erickson* discloses nothing about methods of encryption or about how, where, when, or by whom the data was encrypted. Similarly, in one of the few other references to encrypted data, *Erickson* discloses, "[t]he <DRM> section specifies the DRM mechanism [that was] employed… to package the content. …. [A] local encrypted content blob should be sent to a distant DRM web service for processing, or a remote encrypted content stream should be decrypted by a remote web service" ¶ [25]. Thus, *Erickson* is directed exclusively towards data decryption.

Applicants cannot conceive of how *Erickson* could be said to disclose even a general step of encrypting data, let alone the specific encrypting embodiments claimed in many of Claims 1-23 and 25-31 (discussed in detail below). One of ordinary skill in the art would instinctively appreciate that encryption and decryption typically occur at different times, on different devices, with different purposes, and by different entities.

***Erickson* does not disclose encrypting data as in Claim 1.**

Turning to specific claim rejections, Claim 1 recites as follows:

A method of securing electronic data, the method comprising:
receiving electronic data;
receiving a selection of one of a plurality of digital rights management systems; and

encrypting said received electronic data **in accordance with the selected digital rights management system**.

Thus, Claim 1 is directed towards encrypting electronic data with a selected DRM system, presumably so that digital rights restrictions may be enforced against users. Applicants respectfully submit that *Erickson* does not disclose any sort of "encrypting" step, let alone "encrypting said received electronic data in accordance with the selected digital rights management system," as claimed in Claim 1.

In asserting to the contrary, the Office Action cites to ¶¶ [24-26] of *Erickson*. However, those paragraphs, like the rest of *Erickson*, disclose merely decryption and other operations that may take place on pre-encrypted data. Specifically, ¶¶ [24-26] discuss the format (XML) and content of metadata present in a standardized file wrapper, specifying that the metadata identifies which DRM mechanism was employed when the content was encrypted and contains a reference to a component that can process or decrypt the content. In other words, unlike the invention claimed in Claim 1, *Erickson* is directed towards enabling a user to decrypt and view DRM-protected content, regardless of the DRM mechanism employed.

Concededly, *Erickson's* teachings might be advantageously used in tandem with the elements claimed in Claim 1—it is not difficult to imagine that electronic data encrypted according to Claim 1 might later be wrapped in *Erickson's* "wrapper." However, to anticipate Claim 1, *Erickson* must disclose more than a system that it theoretically compatible with data encrypted according to Claim 1. Indeed, *Erickson* must disclose each and every element of Claim 1, and Applicants respectfully submit that *Erickson* does not meet this standard because it does not disclose "encrypting said received electronic data in accordance with the selected digital rights management system," as claimed in Claim 1. For at least the reasons just discussed, Applicants respectfully submit that Claim 1 is in condition for allowance.

***Erickson* does not disclose each element of Claim 8.**

Applicants respectfully submit that *Erickson* does not anticipate Claim 8 for at least the following reasons. Claim 8 recites as follows:

A method of securely distributing digital content, the method comprising:

receiving a **plurality** of digital data files, the files utilizing a plurality of different file format types;

receiving a selection of a plurality of file format types;

reformatting the files in accordance with the format types;

receiving a **user selection** of a first digital rights management system, the first digital rights management system being one of a plurality of pre-determined digital rights management systems;

encrypting the reformatted files according to the selected digital rights management system; and

transmitting the encrypted files to a **plurality** of consumers.

Erickson, by contrast, is directed towards allowing a single user to decrypt and render a single piece of electronic content at one time:

> a user 10 is sent a secure container 12 containing electronic content.... A generic container handler 15 retrieves details... of the DRM mechanism... and details of the media handler required to handle the data... together with details of how... the required media handler and DRM handler can be obtained.... The content is first passed through the specified DRM handler 14 and then through the specified media handler, such that the sound recording can now be played by the user.

¶ [19]. *Erickson* also discloses various details of the XML metadata used to accomplish the procedure just described. *Erickson* does not anticipate Claim 8 for several reasons.

First, *Erickson* does not disclose "receiving a selection of a **plurality** of file format types; **reformatting** the files in accordance with the format types," as claimed in Claim 8. Rather, *Erickson* discloses receiving a single file in a single format and allowing the user to decrypt and play that file. *Erickson* does not disclose receiving a "plurality" of format types, nor does *Erickson* disclose "reformatting" files.

Second, *Erickson* does not disclose "receiving a **user selection** of a first digital rights management system," as claimed in Clam 8. On the contrary, *Erickson's* DRM system has already been applied to a content file before the file is received by a user.

Third, as discussed above in reference to Claim 1, *Erickson* does not disclose "**encrypting** the reformatted files...," as claimed in Claim 8.

Fourth, *Erickson* does not disclose "**transmitting** the encrypted files to a **plurality** of consumers," as claimed in Claim 8. On the contrary, *Erickson* discloses merely that "a [single] user 10 is sent a [single] secure container 12 containing electronic content." ¶ [19].

For at least the reasons just discussed, Applicants respectfully submit that Claim 8 is in condition for allowance.

***Erickson* does not disclose each element of Claims 11 and 27.**

Claim 11 recites as follows:

> A method of encoding data with one of a plurality of digital rights management systems, the method comprising:
>
> receiving an identifier of an input file, the input file containing input data;
>
> determining a first file format type used in the input data, the first file format type being one of a plurality of pre-determined file format types;
>
> receiving an identifier of a first digital rights management system, the first digital rights management system being one of a plurality of pre-determined digital rights management systems;
>
> retrieving unencrypted data from the input file;
>
> **encrypting the unencrypted data according to the first digital rights management system;**
>
> receiving an identifier of a second file format type for use in an output file, the second file format type being one of a plurality of pre-determined file format types; and
>
> **creating the output file according to the second file format type, wherein the output file contains the encrypted data.**

Claim 27 claims a computer readable medium containing instructions that perform the steps recited in Claim 11. Applicant respectfully submits that Claims 11 and 27 are patentable over *Erickson* for at least the reasons discussed above in reference to Claims 1 and 8. In addition Claims 11 and 27 are further distinguishable from *Erickson* at least because *Erickson* does not disclose "encrypting the unencrypted data" and "creating the output file… contain[ing] the encrypted data," as claimed in Claims 11 and 27.

In asserting to the contrary, the Office Action relies on *Erickson's* disclosure that "a variety of DRM vendors could create 'plug-in' solutions" as "functional extensions to the media **rendering** application." ¶ [15]. As *Erickson* discloses merely plug-ins for **decrypting** DRM protected content prior to rendering, *Erickson* cannot reasonably be read so broadly as to disclose "retrieving unencrypted data from the input file; encrypting the unencrypted data," as claimed in Claims 11 and 27. And *Erickson* certainly cannot reasonably be read to disclose "creating the output file… wherein the output file contains the

encrypted data," as claimed in Claims 11 and 27. Therefore, Applicants respectfully submit that Claims 11 and 27 are in condition for allowance.

***Erickson* does not disclose re-encrypting data, as claimed in Claim 19.**

Claim 19, as currently amended, recites as follows:

> A method of handling secured electronic data, the method comprising:
> receiving electronic data encrypted according to a first digital rights management system;
> **receiving a selection of one a plurality of digital rights management systems to be applied to the data**, wherein the first digital rights management system and the selected digital rights management system are different;
> decrypting said electronic data; and
> re-encrypting said electronic data in accordance with said selected digital rights management system.

Applicant respectfully submits that Claim 19 is patentable over *Erickson* at least for the reasons discussed above. In addition, *Erickson* does not disclose "receiving a selection of one a plurality of digital rights management systems to be applied to the data, wherein the first digital rights management system and the selected digital rights management system are different," as claimed in Claim 19. On the contrary, *Erickson* discloses the existence of only one DRM system, the system that is specified in the <DRM> section of an XML file wrapper, *see, e.g.,* ¶ [24-26], not a first and a selected differing DRM system, as claimed in Claim 19. Furthermore, as discussed at length above, *Erickson* is directed towards decrypting DRM systems that have already been applied to data. Thus, *Erickson* does not disclose "receiving a selection of one a plurality of digital rights management systems to be **applied** to the data," as claimed in Claim 19.

Moreover, upon review of Claim 19, Applicants believe that it did not point out its subject matter as distinctly as might be wished. Claim 19 is therefore presently amended for clarification and now recites the elements of "decrypting said electronic data; and re-encrypting said electronic data in accordance with said selected digital rights management system." While Applicants did not amend Claim 19 in view of the cited reference, Applicants nonetheless believe that the rejection in the Office Action is moot in light of these amendments. Specifically, *Erickson* does not disclose the following elements of Claim 19: "re-encrypting said electronic data in accordance with said selected digital rights

management system." On the contrary, *Erickson* teaches that data is decrypted only when about to be rendered on a client device. *See* ¶ [25]. Thus, according to *Erickson*, there would be no need to ever re-encrypt data in accordance with a selected DRM system, so it is not surprising that *Erickson* does not disclose this element of Claim 19. Accordingly, Applicants respectfully submit that Claim 19 is in condition for allowance.

***Erickson* does not disclose each element of Claim 23.**

Applicant respectfully submits that Claim 23 is patentable over *Erickson* at least for the reasons discussed above. In addition, Claim 23 is further distinguishable from *Erickson* at least because *Erickson* does not disclose the following elements of Claim 23:

> a digital rights management system encryption **library**, accessible by the translation computer, the encryption library comprising a plurality of **classes**, each class configured to create a software module configured to encrypt data according to a particular digital rights management system;
>
> a file format type **library**, accessible by the translation computer, the file format type library comprising a plurality of **classes**, each class configured to create a software module configured to read data using a different file format type;
>
> a file writer **library**, accessible by the translation computer, the file writer library comprising a plurality of **classes**, each class configured to create a software module configured to write to a different file format type; and

In asserting that *Erickson* discloses these elements, the Office Action does not explain its reasoning, merely providing references to the same paragraphs in *Erickson* that have been discussed above.

The terms "library" and "classes" are not specially defined in the specification, so they take their ordinary meaning as would be understood by one of ordinary skill in the art. Specifically, "library" means, "A collection of programs kept with a computer system and made available for processing purposes." Bryan Pfaffenberger, *Webster's New World Computer Dictionary* 214 (10th ed. 2003). "Class" is defined as "a template for building objects that all have the same properties (variables) and methods (functions)." *Id.* at 72. Applicants are unable to readily discern how *Erickson* can possibly be said to disclose the specific libraries, accessible by the translation computer, comprising classes configured to perform the operations claimed in Claim 23. Accordingly, Applicants respectfully submit that Claim 23 is in condition for allowance.

Claims 2-7, 9-10, 12-18, 20-22, 25-26, and 28-31 are allowable at least by dependency.

Claims 2-7, 9-10, 12-18, 20-22, 25-26, and 28-31 are allowable at least because they depend from independent claims that have been shown to be allowable. Moreover, additional distinctions exist between Claims 2-7, 9-10, 12-18, 20-22, 25-26, 28-31 and *Erickson*. Following are a selected number of specific explanations concerning these additional distinctions.

***Erickson* does not anticipate each element of Claims 2, 4-7, 9-10, 12-18, 20-21, 25-26, and 28-30.**

For example, Claims 2 and 20 recite, "the **first and selected digital rights management systems are different**." Similarly, Claims 9, 15-16, 25 and 30 recite, "a **second digital rights management system**." *Erickson*, by contrast, discloses only one DRM system, the system that is specified in the <DRM> section of an XML file wrapper. *See, e.g.,* ¶ [24-26]. Therefore, *Erickson* does not disclose "first and selected digital rights management systems are different," as claimed in Claim 2 and 20, or "a second digital rights management system," as claimed in Claims 9, 15-16, 25 and 30.

For another example, Claims 4-7, 12-14, 21, and 28-29 recite a "compression technique" and/or a "compression format." *Erickson*, however, does not even mention compression techniques or formats. Therefore, *Erickson* does not disclose "compression technique" or "compression format" as claimed in Claims 4-7, 12-14, 21, and 28-29.

In addition, Claim 5 recites "a **consumer selects the digital rights management system** and the compression technique." *Erickson* never discloses that a consumer selects a DRM system. Indeed, *Erickson* is directed towards achieving interoperability, implicitly without requiring any input, knowledge, or selection by the consumer. *See* ¶ [4] (explaining that existing digital protection schemes are too difficult for consumers to use). Therefore, *Erickson* does not disclose "a consumer selects the digital rights management system and the compression technique," as claimed in Claim 5.

For yet another example, Claim 10 recites, "**dynamically creating** at least one of a format object or a writer object corresponding to the file format types of the received files and the selected file format types." *Erickson*, however, discloses nothing about "dynamically

creating" anything, let alone "dynamically creating at least one of a format object or a writer object."

For a further example, Claim 17 recites "generating digital rights management system **rules**, and writing the generated digital rights management system **rules** to the output file." Claim 31 makes an almost identical recitation. Such "rules" are never explicitly defined in the specification, but it is implicit that "rules" are used by a particular DRM system to describe and/or define the limits of access that are allowed to content. *See* ¶ [42]. *Erickson*, however, is directed towards a file wrapper that enables a consumer device to interpret content protected by arbitrary DRM systems. *Erickson* discloses nothing about DRM rules, leaving such details to be implemented elsewhere. On the contrary, the only aspects of a DRM system disclosed by *Erickson* are a type, a handler, and a location. *See* Fig. 2 and associated text. Thus, *Erickson* never even discloses that DRM system rules exist, let alone "generating digital rights management system **rules**, and writing the generated digital rights management system **rules** to the output file," as claimed in Claims 17 and 31.

Similarly, Claim 18 recites, "retrieving digital rights management system **rules** from the input file, (ii) **mapping** the retrieved digital rights management **rules** to rules in accordance with the first digital rights management system, and (iii) writing the **mapped rules** to the output file." Applicants note that very similar elements were deemed to be allowable in Claim 32, and respectfully submit that they are similarly allowable in Claim 18 not only because *Erickson* discloses nothing about DRM system rules (as discussed above), but also because *Erickson* completely fails to disclose **mapping** rules from one DRM system to corresponding rules in another DRM system. Thus, *Erickson* does not disclose "mapping the retrieved digital rights management rules to rules in accordance with the first digital rights management system," as claimed in Claim 18.

For a final example, Claims 25 and 26 each disclose some type of "library comprising a plurality of classes." As discussed above with respect to Claim 23, *Erickson* discloses neither libraries nor classes.

For at least the reasons just discussed, Applicants respectfully submit that *Erickson* does not disclose each and every element of Claims 2, 4-7, 9-10, 12-18, 20-21, 25-26, and 28-30. Accordingly, Applicants respectfully submit that for at least these reasons, the claims are clearly in condition for allowance.

CONCLUSION

For at least the reasons above, Applicants respectfully submit that Claims 1-32 are allowable and request that the Examiner permit these claims to proceed to issuance. Although additional arguments are believed to exist for distinguishing the cited documents, the arguments presented are believed sufficient to address the Examiner's rejections. Likewise, failure of the Applicants to respond to a position taken by the Examiner is not an indication of acceptance or acquiescence of the Examiner's position. Instead, it is believed that the Examiner's positions are rendered moot by the foregoing arguments, and it is therefore not believed necessary to respond to every position taken by the Examiner with which Applicants do not agree.

The Examiner is respectfully requested to contact the undersigned at the telephone number below if there are any remaining questions regarding this Application.

We believe the appropriate fees accompany this transmission. If, however, insufficient fee payment or fee overpayment occurs, the amount may be withdrawn or deposited from/to AXIOS Law Group's deposit account. The deposit account number is 50-4051.

Respectfully submitted,
AXIOS LAW GROUP

Date: April 1, 2008

by: /Adam L.K. Philipp/

Adam L.K. Philipp
Direct: 206.217.2226
E-mail: adam@axioslaw.com
Reg. No.: 42,071

AXIOS Law Group
1525 4th Avenue, Suite 800
Seattle, WA 98101
Telephone: 206-217-2200
Customer No.: 61857